



Qualys Security Conference Dubai

Global IT Asset Management

Siva Mandalam

VP, Product Management, Qualys, Inc.

Qualys Unified IT-IoT-OT Visibility, Analytics and Control Solutions

Visibility

- Managed and unmanaged devices
- Observable and non-observable meta-data
- Hardware, Software, Applications and Traffic

Analytics

- Vulnerability Detection
- Policy Detection
- Threat Quantification

Automated Control

- Remove unauthorized devices
- Policy based automation
- Inline and out-of-band
- Integration with Security and other Qualys tools

Agentless | Agent | Passive | API

Why Visibility?

Digital Transformation drives Endpoint Explosion

IoT/IIoT
Cloud and SaaS
Mobile Devices
Virtualization
BYOD

Digital Transformation

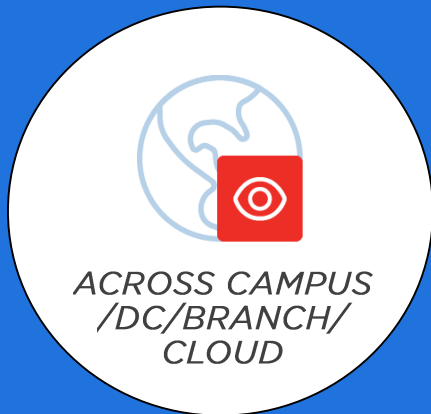


44% of companies
have **5k to 500k**
endpoints

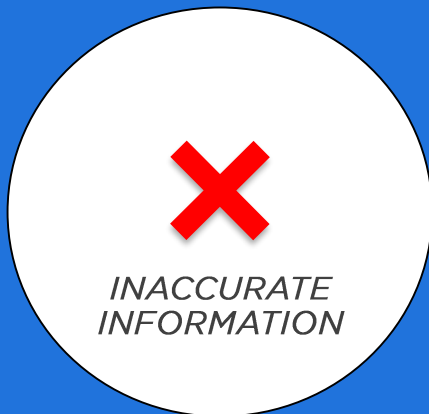
10% of companies have
100k to 500k
endpoints

Challenges with IT Asset Management

VISIBILITY



POINT SOLUTIONS



NO BUSINESS CONTEXT




Agentless vs Agent-based

Agent-based

- Deep-device, software visibility, user info
- Vulnerability Detection
- Policy Compliance
- Threat Quantification
- Suitable for Managed Devices

Agentless

- Device Fingerprinting
- Data Flows
- Application Visibility
- Vulnerability for unmanaged, ICS
- Suitable for unmanaged devices



Both are critical and have a role to play

Introducing Qualys Asset Inventory

Real-time Inventory

Source of truth for IT and Security
teams

Structured and complete context



Benefits



2-second Visibility



Business contextual Inventory

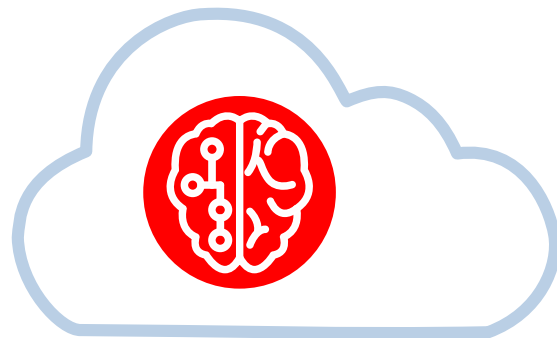
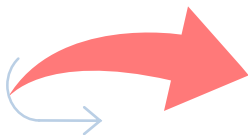


Uniform, accurate information



IT Cost reduction

How is it done?



Physical Scanner

Cloud Agent

Virtual Scanner

Passive Sensor

Cloud Scanner

API

Qualys Sensors

Scalable, Self-updating & Centrally Managed

OS/HW/SW

EoL/EoS

Mfg./owner/product

License type

Market version

Vulnerability/PC

Asset Inventory in Qualys Cloud

Categorization, Normalization, Enrichment

Use case 1: Global IT Visibility

Managed, unmanaged, campus/branch/DC and cloud assets

Inventory every hardware and software

Real-time and contextual info

Manufacturer/Publisher/product/vendor

IP address/MAC address

Major version/version order/service pack/market version

Risk/vulnerability

Policy compliance



The screenshot shows the Qualys Enterprise Asset Inventory dashboard. The top navigation bar includes 'DASHBOARD' and 'INVENTORY'. The main content area displays a summary of '1.10K Total Software Assets' and a list of assets with columns for 'Name', 'Version', 'Risk', and 'Instances'. A green overlay box titled 'Use Case Benefits' is positioned over the right side of the dashboard.

Use Case Benefits

- Illuminate blind spots
- Prioritize security programs
- Control financial risk with unlicensed software
- Rationalize multiple products/versions
- Share context with ITAM tools

Use case 2: Software Inventory with Rich Context

Databases, Applications and Security software agents

Real-time inventory of
managed/unmanaged databases

EoL/EoS status of the software

Market version, multiple version for
software

Report to drive VM programs

Use Case Benefits

- Control financial risk with unlicensed software
- Rationalize multiple products/versions
- Prioritize security programs

Use case 3: Endpoint Devices Visibility

Managed and Unmanaged devices

Automatically discover devices as they enter the network

Get detailed context on

Devices already connected

New devices connecting

Guest/Employee network monitoring

Real-time traffic monitoring

User information

Internet traffic monitoring*



Case Study: Large Bank uses Qualys AI to help Stay Compliant

Customer challenge:

- Monitor unauthorized software
- Find DB versions, EoL/EoS status, market version discrepancies

How do they use it?

- Dashboards to gain global visibility of unauthorized software
- Asset category based search to isolate databases
- Context information to find versions, EoL/EoS status, market version discrepancies



"We have regulatory compliance needs that require us to monitor unauthorized software, current versions of DB software, EoL/EoS software to ensure that we are in compliance "

Chief Information Officer

Case Study: Large Accounting Firm uses Qualys AI for Unified Inventory

Customer challenge:

- Unified global inventory
- Prioritize security needs
- Service Desk optimization

How do they use it?

- Dashboards to gain global visibility
- Asset category based prioritization to drive remediation
- CMDB integration with ServiceNow to drive accurate asset in CMDB

“Single unified inventory management for global assets across 4000 employees and distributed offices are required for us to drive optimizations in internal processes, including vulnerability prioritization, patching/remediation, service desk etc.”

Security Manager

Case Study: Global Technology Leader uses Qualys AI to determine Unmanaged devices

Customer challenge:

Global asset inventory
Unmanaged devices

How do they use it?

- Dashboards to gain global visibility of hardware and software
- Unmanaged devices total to identify all dashboards
- Traffic information from these devices to understand threats and prioritize actions



"We've not been able to understand our devices in its entirety. Qualys AI solution with complete context for devices are excellent way to understand devices, security threats and prioritize actions "

Security Manager

Complete and clean data to your CMDB

Certified ServiceNow App Syncs asset data in both directions.

The screenshot displays the ServiceNow user interface. At the top, the 'service now' logo and 'Service Automation' text are visible. Below the header, a navigation bar shows 'Welcome: Jeff Leggett' with user and lock icons. The left sidebar contains several utility links: 'Toggle Navigator' (ctrl + opt + n), 'List and Form View' (ctrl + opt + v), 'Tagged Documents' (ctrl + opt + t), 'All Bookmarks', and a 'Home' button. The main content area is titled 'Self-Service' and 'Qualys App for ServiceNow CMDB'. Under the 'Configuration' section, there are links for 'API Sources', 'Schedules', 'Properties', 'Sync', 'Advanced', 'Reports', and 'Support'. The 'Sync' link is selected, leading to the 'Sync' configuration page. This page has a 'Schedules' tab. The 'Name' field is set to 'SN_to_Q_Assets', and the 'Active' checkbox is checked. The 'API Source' is 'testing cred', and the 'Sync Direction' is 'Servicenow to Qualys'. The 'Conditional' checkbox is unchecked. Below this, the 'Servicenow to Qualys Sync' section is visible, showing the 'Qualys Asset Tag' as 'ServiceNow' and the 'Table' as 'Computer [cmdb_ci_computer]'. There are buttons for 'Add Filter Condition' and 'Add "OR" Clause'. At the bottom, it states 'All of these conditions must be met' and lists 'IP Address' and 'Fully qualified domain name' as conditions.

Global IT Visibility ▾



Last 30 Days ▾



OPERATING SYSTEM DISTRIBUTION

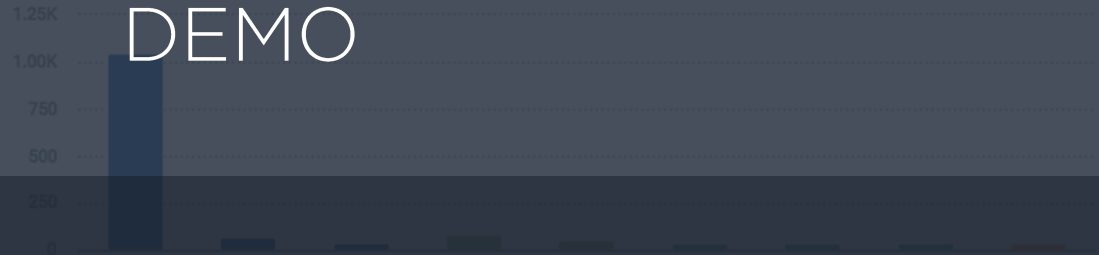
Total

1.44K [view](#)

Windows	1036
Mac	225
Linux	130
Unidentified	26
Virtualization	21

CATEGORY BREAKDOWN

Computers Virtualized Networking Surveillance And Detection Equipment



DEMO

Qualys sensors for complete, detailed asset telemetry
Structuring your inventory (normalization and taxonomy)

Enriching your inventory (e.g. lifecycle)
Blind spots? (showcase passive discovery)

TOP CLIENT OPERATING SYSTEM

PRODUCT	RELEASES	ASSETS
Microsoft Windows 10	1	775
Apple macOS	3	183
Microsoft Windows 7	1	101

TOP CLIENT APPLICATION CATEGORIES

Commercial License Open Source License Unknown



Passive Network Sensor (Beta)

Discovery & Profiling

- Identify and profile devices as soon as they connect to the network
- Continuously enrich existing inventory
- Extends discovery, for sensitive systems



Multi-function Passive Sensor



First Phase (Q2/Q3-2019)

IT asset discovery and profiling
Application recognition and usage

Next (Q4/Q1-2019/20)

Asset discovery and profiling

- SCADA
- Medical Devices

Future use cases

Highlight asset relationship
Traffic anomaly & Network IOC
Smart whitelisting (policies within
Secure Access Control)

Secure Access Control

Use Cases

Grant access to resources only on a need basis

Automated asset attribute processing and enforcement

Limit /Block access (e.g. quarantine) of vulnerable assets or assets out of compliance





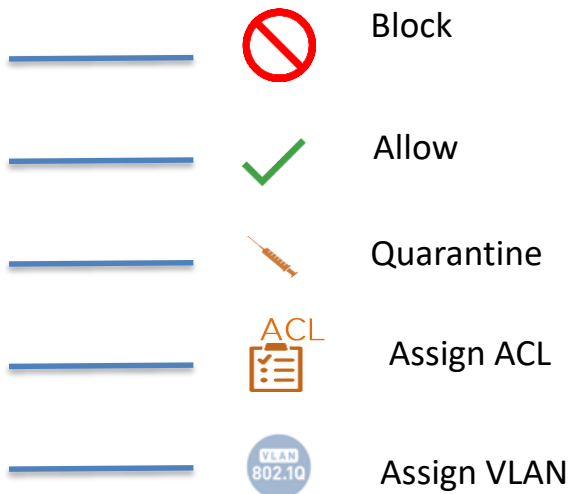
Use Cases

Asset Inventory – Access control using asset inventory attributes



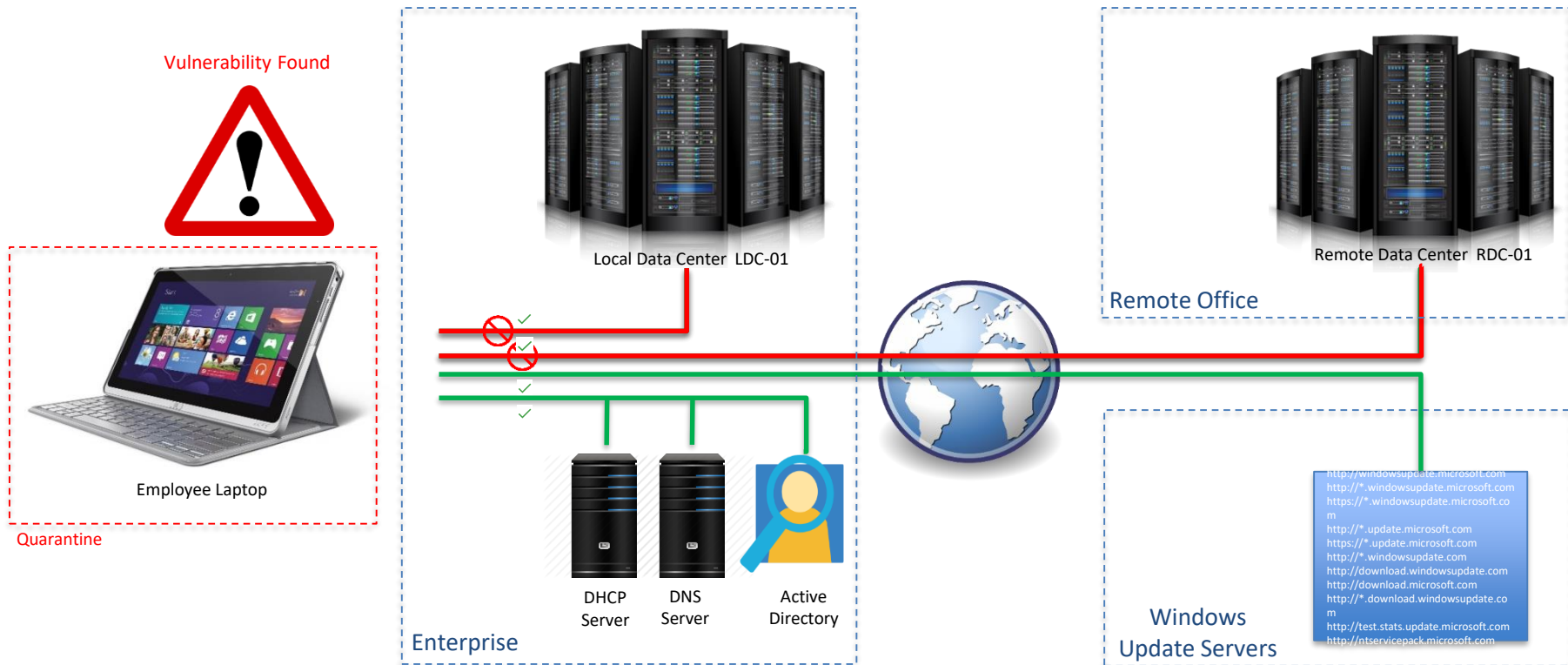
Attributes

System Information
Hardware
Operating System
Services
Network Interfaces
Open Ports
Software Inventory
Software Lifecycle
Secure Zones/subnets



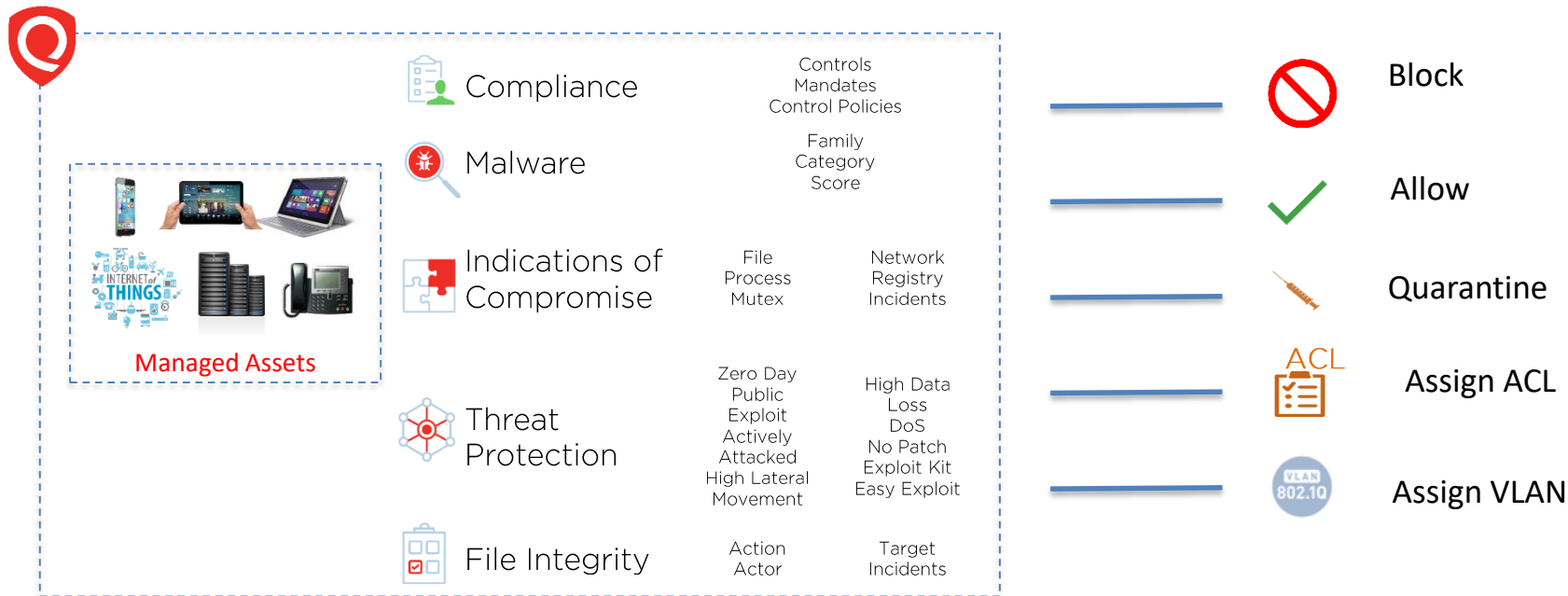
Use Cases

Vulnerabilities – Quarantine assets if vulnerable



Use Cases

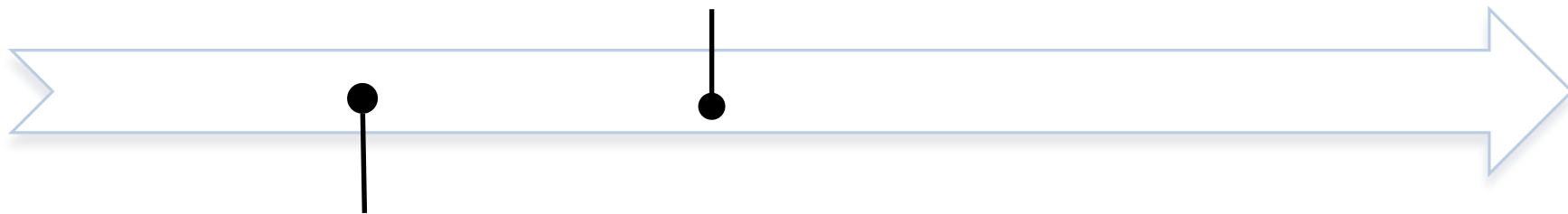
Compliance - Block assets which fail compliance



Secure Access Control

Next Phase (1H'20)

- Public API
- PC and IoC as data source



First Phase (Q4'19/Q1'20)

- Policies using attributes of VM, AI, Asset Tags
- Enforcement Block, Assign VLAN/ACL
- In-line/Out-of-band hybrid operating modes
- Enforcement on SAC appliance or switches

Future use cases

Patch integration
Policy Simulation
Quarantine Notification pop-up
SEM Integration



Qualys Security Conference Dubai

Thank You

SMANDALAM@QUALYS.COM